REMARKS

I. Introduction

Claims 10, 11, and 14-18 remain pending in the present application. In view of the following remarks, it is respectfully submitted that all of the presently pending claims 10, 11, and 14-18 are allowable, and reconsideration of the pending claims is respectfully requested.

II. Rejection of Claims 10, 11 and 14-18 under 35 U.S.C. § 103(a)

Claims 10, 11, and 14-18 stand rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of U.S. Patent No. 5,884,312 ("Dustan") and U.S. Patent No. 6,070,243 ("See"). Applicants respectfully submit that this rejection should be withdrawn for the following reasons.

In rejecting a claim under 35 U.S.C. § 103(a), the Examiner bears the initial burden of presenting a *prima facie* case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). To establish a *prima facie* case of obviousness, the Examiner must show, *inter alia*, that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify or combine the references, and that, when so modified or combined, the prior art teaches or suggests all of the claim limitations. M.P.E.P. §2143. In addition, as clearly indicated by the Supreme Court, it is "important to identify a reason that would have prompted a person of ordinary skill in the relevant field to [modify] the [prior art] elements" in the manner claimed. See KSR Int'l Co. v. Teleflex, Inc., 82 U.S.P.Q.2d 1385 (2007). In this regard, the Supreme Court further noted that "rejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." Id., at 1396. To the extent that the Examiner may be relying on the doctrine of inherent disclosure in support of the obviousness rejection, the Examiner must provide a "basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristics necessarily flow from the teachings of the applied art." (See M.P.E.P. § 2112; emphasis in original; see also Ex parte Levy, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990)).

Claim 10 recites the following:

10. A system for access authorization, comprising:

a base device including a computer, wherein **the base device initially transmits a prompt signal** within a framework of an initial prompt/reply cycle that is successfully carried out, and wherein the prompt signal is stored in the base device; and

at least one **remote control storing the initially transmitted prompt signal** from the initial prompt/reply cycle;

wherein, in an **access authorization process** during system operation **subsequent to the previous, initial prompt/reply cycle that is successfully carried out**, the at least one remote control transmits to the base device a code word containing a reply, **the reply being formed at least partially as a function of the prompt signal stored in the at least one remote control**, wherein the base device receives the code word containing the reply and compares the reply contained in the code word with a required reply, **the required reply being formed at least partially as a function of the prompt signal stored in the base device**, wherein an access is authorized if the reply contained in the code word agrees with the required reply, and wherein **the prompt signal stored in the base device is erased when a number of failed agreements of the reply and the required reply exceeds a specifiable limiting value**.

In support of the rejection, the Examiner contends the following: a) Dustan teaches transmitting "**a prompt** within the framework of **an initial successful prompt/reply cycle** (SSL, column 11, lines 49-60) where **the prompt** is stored in the base station (**session key of SSL**), and a remote control device **(client)** which stores **the prompt (session key of SSL)**"; b) Dustan further teaches "**subsequent to the initial prompt/reply cycle**, the remote control device (client) transmits **a reply** (column 8, lines 63-66) to the base device (database server) partially [as] **a function of the initial prompt** (**SSL session key**, column 9, lines 3-8)"; and c) "the base station receives the reply and compares it with the required reply (column 9, lines 1-3)." To the extent the Examiner is arguing that the **"session key"** generated as part of an **SSL session** satisfies the claimed limitation of "a prompt" as recited in claim 10, Applicants note that the Examiner's interpretation is implicitly and entirely based on the Examiner's opinion and/or the general knowledge available in the art, since the cited prior art references do not mention anything relating to the specific features of SSL, let alone the

"session key of SSL."[1] To the extent the Examiner is relying entirely on the Examiner's own opinion and/or the implicitly alleged general knowledge available in the art, the Examiner should provide documentary evidence to support the Examiner's assertions. In any case, applying the general knowledge available in the art, however, it is readily apparent that the Examiner's asserted interpretation does not make any sense, as explained in detail below.

First, to the extent the Examiner is contending that the **"session key of SSL"** is equivalent to the claimed **"prompt signal"** which is initially **transmitted by the base device** "within a framework of an initial prompt/reply cycle that is successfully carried out," it is widely known that the **"session key"** of SSL is the **end product** of the SSL **handshake** protocol, which handshake is **initiated by the client**, not the server. Second, it is also widely known that the "session key of SSL" is not transmitted by the server to the client (indeed, the **non-transmission** of the ultimate "session key" is the core security benefit); instead, **the "session key of SSL" is the end product which is independently derived by both the client and the server**. The detailed operation for generating the session key is as follows: the client initially creates a "pre-master secret" which is sent to the server; the client and the server use the pre-master secret to independently generate a "master secret"; and both the client and the server use the master secret to **independently generate the session keys**, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session. For at least these reasons, there is no reasonable basis to contend that "the session key of SSL" is in any way equivalent to the claimed **"prompt signal"** which is initially **transmitted by the base device** "within a framework of an initial prompt/reply cycle that is successfully carried out."

In addition to the above, the Examiner makes the following contentions in support of the asserted combination of the teachings of Dustan and See: a) "Dustan does not disclose erasing the SSL session key after number of failed attempts"; b) "See discloses terminating a session with a user after a predetermined number of failed login attempts"; and c) "[i]t would have been obvious for one of ordinary skill in the art to use the method of See to delete the SSL session key of Dustan after a number of failed attempts as to not allow a hacker unlimited attempts to break into the system." However, the Examiner's contentions are based

[1] Col. 9, l. 1-11 of Dustan mentions a "session id" which is generated upon verification of the user's account number and password by the server 22, so it is clear that the "session id" of Dustan is completely unrelated to the "session key" of SSL asserted by the Examiner.

on clearly incorrect commingling of different and unrelated concepts, and the overall combination simply does not make sense. Most fundamentally, the notion of "erasing the SSL session key **after number of failed attempts**" doesn't make any sense because the SSL session key is established **only if the SSL handshake is successfully completed**, and the **SSL handshake (and thus the SSL session) is ended without any generation of the SSL session key** upon initial failure to authenticate, i.e., there is no **possibility of repeated failed attempts** to authenticate within the SSL handshake protocol. In addition, the "predetermined number of failed login attempts" of See relates to **attempts to authenticate user identification information (the log-in response)**, which has nothing to do with SSL handshake or SSL session key allegedly implied in Dustan. Accordingly, in view of the overall teachings of Dustan and See, the Examiner's assertion that it would have been "obvious for one of ordinary skill in the art to use the **method of See to delete the SSL session key of Dustan** after a number of failed attempts" simply doesn't make any sense.

Independent of the above, the combination of Dustan and See does not disclose, or even suggest, the feature that **in an access authorization process** during system operation **subsequent to the previous, initial prompt/reply cycle** that is successfully carried out, **the prompt signal stored in the base device is erased** when a number of failed agreements of the reply and the required reply exceeds a specifiable limiting value. In this regard, See merely indicates **terminating the initial authentication session (i.e., initial prompt/reply cycle)** after a configurable number of failed log-in attempts, (e.g., col. 11, lines 30-38), but not during system operation subsequent to the previous, initial prompt/reply cycle that is successfully carried out, as recited in claim 10.

For at least the foregoing reasons, the overall teachings of Dustan and See cannot render claim 10 and its dependent claims 11 and 14-18 unpatentable. Withdrawal of the obviousness rejection is respectfully requested.

CONCLUSION

Applicants respectfully submit that all pending claims of the present application are now in condition for allowance. Prompt reconsideration and allowance of the present application are therefore earnestly solicited.

Respectfully submitted,

(R. No. 36,197)

Dated: January 12, 2009

By: Jong Lee for Gerard Messina
Gerard A. Messina
Reg. No. 35,952

KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200

CUSTOMER NO. 26646